

HAVN

INTERNET AND ACCEPTABLE USE POLICY

Published at www.joinhavn.com/internet-policy

1. Scope, Locations, and Acceptance

This Internet and Acceptable Use Policy (this “Policy”) governs all access to and use of the internet, wired and wireless network, telecommunications systems, and related infrastructure (collectively, the “Network”) at every location operated or managed by HAVN, including:

(a) Salt Lake Crossing, LLC commonly known as “HAVN SLX”, located at 470 W 200 N, Salt Lake City, UT 84103.

(b) The Sanctuary at Lehi, LLC commonly known as “HAVN Sanctuary”, located at 2777 North Sandalwood Drive, Lehi, UT 84043.

together with any other location now or hereafter operated or managed under the HAVN name or by any HAVN affiliate (each, a “Location,” and collectively, the “Locations”).

“HAVN,” “we,” and “us” mean Salt Lake Crossing, LLC, The Sanctuary at Lehi, LLC, and each of their respective parents, subsidiaries, affiliates, and successors, and any other entity that operates or manages a Location.

This Policy applies at all Locations and to every member, licensee, authorized user, employee, contractor, guest, invitee, and any other person or device that accesses the Network at any Location (each, a “User”), regardless of which entity the User contracts with. A User whose agreement is with one HAVN entity remains subject to this Policy when accessing the Network at any other Location.

Where a User accesses the Network under a membership, license, or occupancy agreement with any HAVN entity (an “Agreement”), this Policy is incorporated into and forms part of that Agreement. Each member or licensee is responsible for the compliance of all of its authorized users, employees, contractors, guests, and invitees, and any act or omission by those persons is deemed an act or omission of that member or licensee.

Accessing the Network at any Location constitutes acceptance of this Policy. If a User does not agree to this Policy, that User must not access the Network.

2. Definitions

“Network” has the meaning given in Section 1 and includes, at each Location, all HAVN-provided internet access, wired ports, wireless access points, switches, routers, firewalls, cabling, patch panels, telecommunications closets, VLANs, IP address assignments, and any HAVN-provided printers, displays, conference room technology, access control systems, or other connected equipment.

“User Equipment” means any device or system owned, leased, controlled, or introduced by a User that connects to or interacts with the Network, including computers, servers, network-attached storage, cameras, sensors, phones, printers, routers, switches, access points, and any other hardware.

“Content” means any data, communication, file, message, transmission, or material sent, received, stored, uploaded, downloaded, or accessed through the Network.

3. Nature of the Service

The Network is provided as a shared amenity for ordinary business use. It is a commercial-grade shared internet connection and is not a dedicated circuit, a private line, or a managed IT service.

HAVN does not provide, and expressly disclaims, any of the following unless separately agreed in a written, signed addendum: guaranteed bandwidth, guaranteed uptime, a service level agreement, network monitoring on a User's behalf, IT support, help desk services, endpoint management, data backup, disaster recovery, business continuity, static IP addresses, port forwarding, inbound routing, or dedicated hardware.

HAVN may modify, upgrade, reconfigure, throttle, segment, restrict, suspend, or discontinue any part of the Network at any Location at any time, with or without notice.

4. Access Credentials and Accounts

Network credentials, including wireless passphrases, certificates, VPN credentials, and any account issued by HAVN, are provided for the exclusive use of the authorized User to whom they are issued.

Users must not:

- (a) share, publish, post, transmit, sell, resell, sublicense, or otherwise disclose Network credentials to any person who is not an authorized User under an active Agreement;
- (b) permit any third party to access the Network through the User's credentials or User Equipment;
- (c) attempt to access the Network using credentials issued to another User; or
- (d) circumvent, disable, or attempt to defeat any authentication, captive portal, device registration, network access control, or session limit imposed by HAVN.

HAVN may limit the number of concurrent devices per User, require device registration, require periodic credential rotation, and revoke credentials at any time. Users must notify HAVN immediately upon learning that credentials have been lost, shared, or compromised.

5. Prohibited Conduct

Users must not use the Network, and must not permit the Network to be used, for any of the following:

5.1 Unlawful Activity

- (a) Any activity that violates any applicable federal, state, local, or foreign law, regulation, ordinance, court order, or the rights of any third party.
- (b) Transmitting, storing, distributing, or accessing any material that is unlawful, including child sexual abuse material, material that facilitates human trafficking, or material subject to export control restrictions transmitted in violation of those restrictions.
- (c) Fraud, phishing, identity theft, money laundering, unlawful gambling, or the sale or distribution of controlled substances, firearms, or other regulated goods in violation of law.

5.2 Security Violations and Unauthorized Access

- (a) Accessing or attempting to access any computer, device, account, data, or network resource without authorization, including the systems of other Users of the Network.

- (b) Port scanning, network scanning, vulnerability scanning, enumeration, fingerprinting, or probing of any host, device, or network segment that the User does not own or is not expressly authorized in writing by the owner to test.
- (c) Packet sniffing, traffic interception, wireless monitoring, promiscuous-mode capture, or any attempt to intercept, monitor, or capture data not intended for the User.
- (d) IP spoofing, MAC address spoofing, ARP poisoning, DNS poisoning or hijacking, DHCP spoofing, rogue DHCP servers, man-in-the-middle attacks, session hijacking, or any technique that misrepresents the origin of traffic or a device's identity on the Network.
- (e) Deploying, operating, or attempting to operate any rogue access point, evil twin, deauthentication tool, jammer, signal interference device, or any device or software intended to disrupt, degrade, or interfere with wireless service.
- (f) Introducing or distributing malware, ransomware, viruses, worms, trojans, keyloggers, rootkits, spyware, botnet clients, command-and-control infrastructure, or any other malicious code.
- (g) Conducting or facilitating any denial of service or distributed denial of service attack, amplification attack, brute force attack, credential stuffing, or password cracking, whether directed at the Network or at any third party.
- (h) Circumventing, disabling, or tampering with any firewall, filter, VLAN segmentation, access control list, logging mechanism, or other security control implemented by HAVN.
- (i) Conducting penetration testing, red team exercises, security research, or offensive security operations of any kind using the Network, except against systems the User owns and only with HAVN's prior written consent.

5.3 Cryptocurrency Mining and Excessive Resource Consumption

- (a) Cryptocurrency mining, coin minting, hashing, staking validation requiring sustained compute, blockchain node operation, distributed computing projects, or any similar activity, whether conducted on User Equipment or by causing any other device to perform such activity, is strictly prohibited at all Locations, on and off the Network.
- (b) Operating GPU clusters, mining rigs, ASIC hardware, sustained high-draw compute equipment, or any equipment whose primary function is sustained computational processing is prohibited without HAVN's prior written consent, and HAVN may condition consent on separately metered power, additional cooling, additional fees, or all of the foregoing.
- (c) Any activity that consumes bandwidth, power, cooling, or Network resources in a manner that, in HAVN's sole determination, is disproportionate to ordinary business use or degrades the experience of other Users.

5.4 Bandwidth and Traffic Abuse

- (a) Operating public-facing servers, file servers, streaming servers, game servers, media servers, proxy servers, Tor exit nodes, open relays, or open resolvers on the Network.
- (b) Peer-to-peer file sharing, torrenting, or seeding, except where the User can demonstrate the traffic

is entirely lawful and does not involve infringing material.

(c) Sustained bulk data transfers, continuous backup or synchronization jobs, large-scale scraping or crawling, automated download tools, or bandwidth-saturating processes conducted during business hours without HAVN's prior written consent.

(d) Reselling, resharing, redistributing, sublicensing, or extending Network access to any person or premises outside the User's licensed space, including by bridging, tethering, repeating, extending, or rebroadcasting the Network.

5.5 Abusive Communications and Content

(a) Sending unsolicited bulk email, spam, chain messages, or commercial messages in violation of the CAN-SPAM Act or any other applicable law.

(b) Harassment, stalking, threats, defamation, doxxing, or any communication that would violate HAVN's community, anti-harassment, or house rules.

(c) Viewing, displaying, or transmitting sexually explicit, obscene, violent, or otherwise offensive material in any location where it is visible or audible to others, including through open office doors, glass-walled offices, and shared monitors.

(d) Impersonating any person or entity, or falsely representing an affiliation with HAVN or any other person.

5.6 Intellectual Property

(a) Downloading, uploading, streaming, storing, or distributing any material in violation of any copyright, trademark, patent, trade secret, license, or other intellectual property right.

(b) Circumventing technological protection measures or digital rights management controls.

6. Network Infrastructure and Private Office Installations

This Section applies with particular force to members with private offices, private suites, or dedicated space in which User Equipment is installed.

6.1 HAVN Infrastructure Is Off Limits

Users must not access, open, enter, alter, move, unplug, reconfigure, re-cable, patch, repatch, or otherwise interfere with any HAVN telecommunications closet, network rack, switch, router, firewall, access point, patch panel, cabling, conduit, or demarcation point. These areas and components are restricted to HAVN and its authorized vendors.

6.2 No User-Installed Network Equipment Without Consent

Users must not connect any of the following to the Network without HAVN's prior written consent: routers, switches, hubs, wireless access points, wireless repeaters or extenders, mesh nodes, firewalls, VPN concentrators, network-attached storage, servers, IoT gateways, or any device that provides addressing, routing, switching, or wireless broadcast functions.

A User's own equipment that operates entirely behind a single Network port and does not provide DHCP, routing, or wireless services to any device outside the User's licensed space may be permitted at HAVN's discretion.

6.3 Cabling and Physical Work

Users must not run, pull, terminate, drill for, or install any cabling, conduit, wall plate, mount, or penetration of any kind. All cabling requests, additional drops, port activations, and physical infrastructure changes must be submitted to HAVN and will be performed by HAVN or its designated vendor, at the User's expense where HAVN determines the work is for the User's exclusive benefit.

6.4 Wireless Interference

Users must not operate any device that materially interferes with HAVN's wireless spectrum, including unauthorized access points broadcasting on HAVN's channels, high-power transmitters, wireless bridges, or radio equipment operating in the 2.4 GHz, 5 GHz, or 6 GHz bands in a manner that degrades Network performance. HAVN may require any interfering device to be powered down or removed.

6.5 Private Circuits

A User may not install a separate internet circuit, dedicated line, fixed wireless antenna, satellite receiver, or other telecommunications service at any Location without HAVN's prior written consent, which may be conditioned on carrier selection, routing, installation method, cost allocation, restoration obligations, insurance, and additional fees.

6.6 Cameras and Recording Devices

Users must not install or operate any camera, microphone, or recording device that captures any common area, corridor, another member's space, or any area outside the User's licensed premises. Any camera installed within a User's licensed premises must be disclosed to HAVN in advance and must comply with all applicable law regarding notice and consent.

6.7 Removal and Restoration

All User Equipment must be removed at the end of the User's Agreement, and the space and any HAVN infrastructure must be restored to its original condition. Equipment left behind may be removed and disposed of by HAVN at the User's expense. HAVN is not responsible for any data on abandoned equipment.

7. User Equipment and Security Obligations

Each User is solely responsible for the security, configuration, patching, maintenance, and lawful operation of its own User Equipment, systems, accounts, and data.

At minimum, each User accessing the Network must:

- (a) maintain currently supported operating systems and applications with security updates applied on a reasonable schedule;
- (b) run reputable endpoint protection on all devices where such protection is commercially available;
- (c) enable device-level authentication, screen locks, and, where available, full disk encryption;
- (d) change all default credentials on any device connected to the Network, including printers, cameras, IoT devices, and network hardware;
- (e) use its own VPN or encrypted transport for any sensitive traffic, and not rely on the Network to provide confidentiality;
- (f) maintain its own backups of all data, on its own media or its own cloud services; and

(g) promptly disconnect and remediate any device that is infected, compromised, or generating abusive traffic. HAVN may quarantine, block, rate-limit, or disconnect any User Equipment that HAVN reasonably believes is compromised, misconfigured, generating malicious or abusive traffic, or degrading the Network, without prior notice and without liability.

8. Monitoring, Logging, and No Expectation of Privacy

The Network is a shared commercial network. Users have no expectation of privacy in any use of the Network.

HAVN and its vendors may monitor, log, inspect, record, retain, and analyze Network traffic, metadata, connection logs, DNS queries, device identifiers, MAC addresses, IP assignments, bandwidth utilization, session duration, and access point associations for purposes including security, capacity planning, troubleshooting, abuse detection, enforcement of this Policy, and compliance with law.

HAVN may deploy filtering, DNS-level blocking, intrusion detection and prevention, geoblocking, and traffic shaping. HAVN does not undertake, and expressly disclaims, any obligation to filter, monitor, or block any particular content, traffic, or threat, and no filtering that HAVN elects to deploy creates any duty to any User.

By accessing the Network, each User consents to the monitoring, logging, and interception described in this Section, on its own behalf and on behalf of all of its authorized users, employees, contractors, and guests, and represents that it has obtained any consent from those persons that applicable law requires. Members and licensees are responsible for notifying their own personnel of this Section.

HAVN retains Network logs for approximately [90] days in the ordinary course, and may retain logs longer where required by law, requested by law enforcement, or relevant to an investigation, dispute, or legal hold.

9. Regulated and Sensitive Data

The Network is a general-purpose shared network. It is not certified, audited, assessed, or represented as compliant with any regulatory or industry framework, including HIPAA, PCI DSS, SOC 2, ISO 27001, FedRAMP, CJIS, ITAR, EAR, GLBA, FERPA, CMMC, or DFARS.

HAVN is not a business associate, subprocessor, subcontractor, or covered entity with respect to any User's data, and providing Network access does not create any such relationship. HAVN will not execute a business associate agreement, data processing agreement, or compliance attestation as a condition of providing Network access.

Any User that transmits, processes, or stores protected health information, cardholder data, controlled unclassified information, export-controlled technical data, financial account data, biometric data, or other regulated or sensitive data does so at its own risk and is solely responsible for implementing whatever segmentation, encryption, tokenization, access controls, and compensating controls its obligations require. HAVN recommends that any such User use its own encrypted tunnel and its own security controls end to end.

10. Copyright, DMCA, and Infringement Notices

HAVN may receive notices of alleged copyright infringement from upstream providers, rights holders, or their agents relating to traffic originating from the Network. Upon receipt of such a notice, HAVN may take any of the following actions: forward the notice to the responsible member or licensee; require the member

or licensee to identify the responsible device or user; require immediate cessation of the conduct; suspend or terminate Network access for the responsible device, user, or member; and respond to the complaining party.

Members and licensees are responsible for responding to notices attributable to their traffic and for the acts of all of their authorized users. Repeat infringers will have Network access terminated.

Notices of claimed copyright infringement should be directed to HAVN's designated agent at the address in Section 20 and must contain the elements required by 17 U.S.C. § 512(c)(3).

11. Guests and Visitors

Guest Network access, where offered, is provided as a courtesy, is segregated from member traffic, may be time-limited and bandwidth-limited, and is subject to this Policy in full.

Members and licensees are responsible for the conduct of their guests on the Network and must not provide guests with member credentials. Guests must use the designated guest network.

Users may not permit any person under 18 years of age to access the Network unsupervised, and the supervising member is responsible for that person's use.

12. Voice, Video, and Emergency Services

HAVN does not provide voice service. Any VoIP, softphone, or unified communications service a User operates over the Network is the User's own service, obtained from the User's own provider.

HAVN makes no representation that VoIP, video conferencing, or any real-time application will function on the Network at any given quality level, and HAVN does not provide quality of service guarantees.

Users relying on VoIP for emergency calling are solely responsible for registering an accurate physical address with their provider and for maintaining an alternative means of contacting emergency services. HAVN is not responsible for any failure of emergency calling over the Network.

13. Reporting Obligations

Users must promptly notify HAVN at privacy@joinhavn.com upon becoming aware of:

- (a) any actual or suspected compromise of Network credentials or User Equipment connected to the Network;
- (b) any security incident, malware infection, or unauthorized access originating from or affecting the User's Network use;
- (c) any vulnerability, misconfiguration, or exposure the User observes in the Network; and
- (d) any conduct by another User that the User believes violates this Policy.

Users must not investigate, test, or exploit any suspected vulnerability in the Network.

14. Enforcement

HAVN may investigate any suspected violation of this Policy and may take any action it deems appropriate, in its sole discretion, with or without prior notice, including:

- (a) suspending, throttling, quarantining, or terminating Network access for any device, user, member, or licensee;

- (b) blocking specific traffic, ports, protocols, domains, or destinations;
- (c) removing or requiring removal of User Equipment;
- (d) requiring remediation as a condition of restored access;
- (e) charging the responsible member or licensee for HAVN's costs of investigation, remediation, replacement equipment, professional services, and any third-party claims, fines, or penalties arising from the violation;
- (f) terminating the User's Agreement in accordance with its terms; and
- (g) referring the matter to law enforcement.

Suspension or termination of Network access under this Policy does not relieve any member or licensee of any payment obligation under its Agreement, and does not entitle any member or licensee to any credit, abatement, refund, or offset.

HAVN's failure to enforce any provision of this Policy in any instance is not a waiver of that provision or of HAVN's right to enforce it later.

15. Cooperation with Legal Process

HAVN may disclose Network logs, User information, device identifiers, traffic records, and any other information in its possession to law enforcement, regulators, courts, or other governmental authorities in response to a subpoena, warrant, court order, or other legal process, or where HAVN believes in good faith that disclosure is necessary to protect the rights, property, or safety of HAVN, its members, or the public.

Users agree to cooperate reasonably with any investigation or legal proceeding relating to Network use, and HAVN is under no obligation to notify a User in advance of any such disclosure except where required by law.

16. Indemnification

Each member and licensee will indemnify, defend, and hold harmless each HAVN entity, whether or not it is a party to that member's or licensee's Agreement, and each of their respective owners, managers, members, officers, employees, agents, contractors, and property owners and landlords, from and against any and all claims, demands, actions, damages, losses, liabilities, fines, penalties, judgments, settlements, and expenses, including reasonable attorneys' fees and costs of investigation and remediation, arising out of or relating to:

- (a) any use of the Network by the member, licensee, or any of its authorized users, employees, contractors, guests, or invitees;
- (b) any violation of this Policy;
- (c) any claim of copyright or other intellectual property infringement attributable to the member's or licensee's traffic;
- (d) any security incident, data breach, or unauthorized disclosure involving the member's or licensee's data, systems, or User Equipment; and
- (e) any claim by any third party arising from the member's or licensee's Network use.

This obligation survives termination or expiration of the applicable Agreement.

17. Disclaimers and Limitation of Liability

THE NETWORK IS PROVIDED “AS IS” AND “AS AVAILABLE,” WITH ALL FAULTS AND WITHOUT WARRANTY OF ANY KIND. HAVN DISCLAIMS ALL WARRANTIES, EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, INCLUDING ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, ACCURACY, SECURITY, RELIABILITY, OR UNINTERRUPTED OR ERROR-FREE OPERATION.

HAVN MAKES NO REPRESENTATION WHATSOEVER AS TO THE SECURITY OF THE NETWORK. USE OF THE NETWORK IS AT EACH USER’S SOLE RISK. EACH USER IS SOLELY RESPONSIBLE FOR PROTECTING ITS COMPUTERS, DEVICES, SOFTWARE, DATA, INFORMATION, BUSINESS OPERATIONS, AND GOODWILL FROM DAMAGE, LOSS, UNAUTHORIZED ACCESS, VIRUSES, MALWARE, RANSOMWARE, AND OTHER CYBERSECURITY THREATS.

HAVN WILL NOT BE LIABLE FOR ANY LOSS OF DATA, INFORMATION, BUSINESS OPPORTUNITIES, GOODWILL, PROFITS, OR REVENUE, OR FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, EXEMPLARY, OR PUNITIVE DAMAGES, ARISING FROM OR RELATING TO ANY INTERRUPTION, FAILURE, DEGRADATION, LATENCY, UNAVAILABILITY, INTERCEPTION, COMPROMISE, OR MISUSE OF THE NETWORK, OR FROM THE ACTS OR OMISSIONS OF ANY OTHER USER, REGARDLESS OF THE THEORY OF LIABILITY AND EVEN IF HAVN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Nothing in this Policy expands HAVN’s liability beyond what is set forth in the applicable Agreement, and the limitations of liability in the applicable Agreement apply to this Policy in full.

18. Changes to This Policy

HAVN may amend this Policy at any time by posting a revised version at www.joinhavn.com/internet-policy. The revised Policy is effective upon posting, or on such later date as HAVN specifies. Continued use of the Network after the effective date constitutes acceptance. Users are responsible for reviewing this Policy periodically.

19. Order of Precedence

In the event of a conflict between this Policy and a member’s or licensee’s Agreement, the Agreement controls, except that where this Policy imposes a stricter or additional obligation on the User, the stricter obligation applies.

With respect to any member or licensee, the Agreement referenced in this Policy is the agreement between that member or licensee and the HAVN entity operating the applicable Location. This Policy applies uniformly across all Locations, but no HAVN entity assumes any obligation under another HAVN entity’s Agreement by reason of this Policy.

20. Contact

General and security matters: privacy@joinhavn.com